

Oracle Blockchain Cloud Service

架构及其应用开发

Agenda

- 区块链简介
- Hyperledger Fabric架构
- Oracle区块链云简介
- Oracle区块链开发

Agenda

- 区块链简介
- Hyperledger Fabric架构
- Oracle区块链云简介
- Oracle区块链开发



正常人能不能参与区块链？

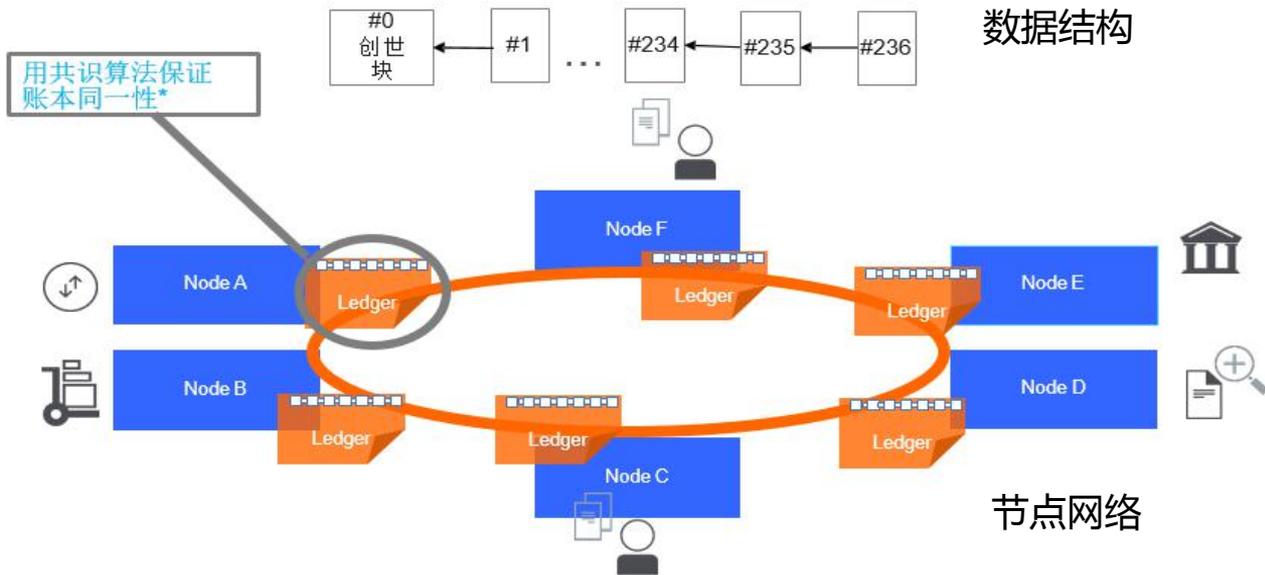
- **公链**  **联盟链** **币圈**  **链圈**
- 流行病在公链上的币圈
- 技术天才在发明各种链
- 正常人在做联盟链技术

**对，正常人（佛系屌丝）在安静地做企业级联盟链应用
Hyperledger Fabric为此而生**

在这之前...

什么是区块链?

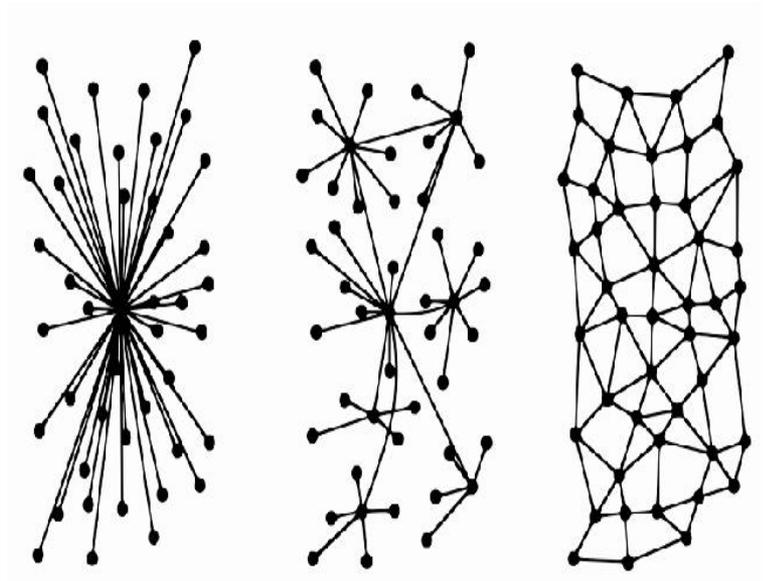
- 就是一个区块的链（废话）**顺序的** **被hash的** **交易数据的链**
 - 每个区块包含多条已排序的交易
 - 区块链建立一个所有的有序地交易链



- **公链--真正的完全去中心的区块链**
 - 用户不用注册就能匿名参与的链，无需授权就能访问网络的区块链。
 - 公链的任何区块对外公开，任何人都可以发送价值。
 - 比特币以太坊是著名公链，公链适合玩币，使人疯狂。
- **联盟链--行业内的可监管区块链**
 - 联盟链仅限于联盟成员参与，成员参与区块链运行需要按照规则获取读写记账的权限。
 - 成员需要注册才可使用。
- **私有链--机构内私有定制区块链**
 - 私有链仅在机构内使用，读写权，记账权由组织内自由定制。
 - 央行发行的数字货币就是私有链。
- **侧链--与比特币挂钩，能和比特币区块链交互的区块链**
- **跨链，上链，链上，链下...**

- 节点 (参与者) 需要许可才能参与到区块链网络
- 动机
 - 企业应用和分布式账本技术 distributed ledger technology (DLT)
 - 提升公链的性能：比特币10分钟出块；以太坊15秒，然而经常阻塞。
- 对于企业应用来说
 - 参与者通常都需要能够识别其他参与者
- 联盟链实现: Chain, Qurum, Tendermint, Ripple, 和.....Hyperledger Fabric

- **为什么去中心？**
 - 中心化的缺点：脆弱，不透明
 - 中介机构在这中间赚各种钱
- **为什么能去中心？**
 - 分布式技术
 - 密码学
 - 博弈论
- **去中心后的商业模式？**
 - 本质是去中介
 - 开放，共享，去中介
- **具体来说...**





去中心后的用例



区块链应用场景概览

区块链演化(2009-至今)

2009
Bitcoin



- 硬编码的加密货币程序，有限的基于堆栈的脚本语言
- Proof-of-work (POW) 共识
- 原生加密货币(BTC)
- 公链，匿名加入

区块链 1.0

2014
Ethereum



- Dapps (智能合约) ，专门的语言 (Solidity)
- Proof-of-work (POW) 共识
- 原生加密货币 (ETH)
- 公链

区块链 2.0

2017
Hyperledger
Fabric



- Dapps (chaincodes) ，可以使用通用语言编写(e.g., golang, Java)
- 模块化/可插拔的共识
- 去掉原生货币
- 多实例部署
- 联盟链

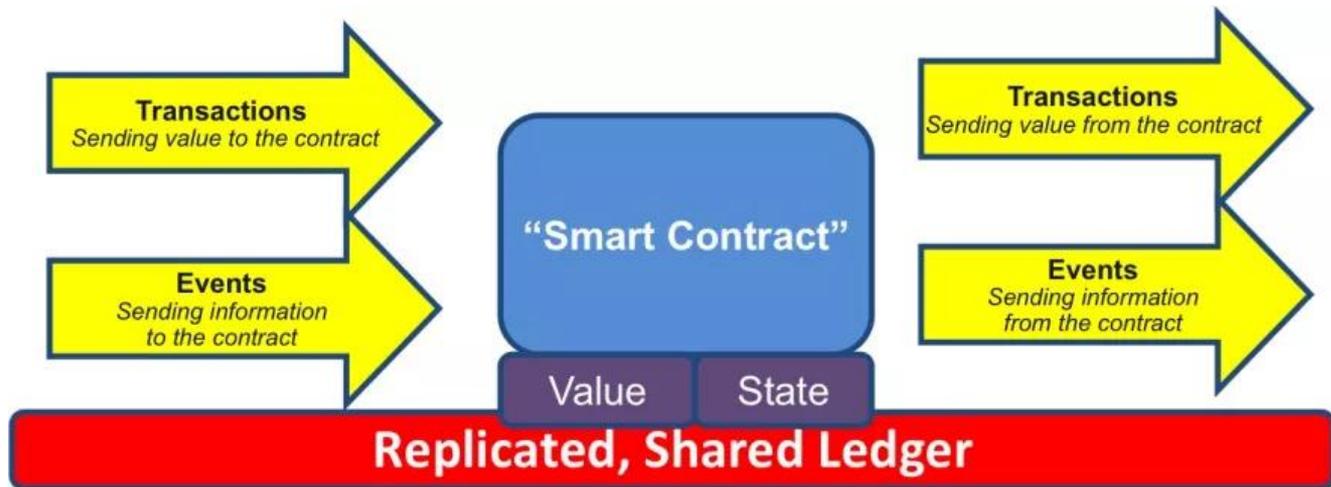
区块链 3.0



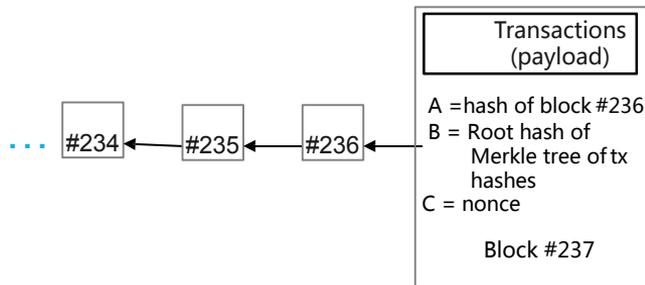
区块链交易和分布式应用 (Dapps)

- 比特币交易
 - 简单的虚拟货币转移
- 交易可以不简单，也可以不和加密货币相关
 - Dapps
 - 智能合约 (Ethereum) 或者 链码 (Hyperledger Fabric)
- *A smart contract is an event driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger. [Swanson2015]*

“智能合约” -> (复制) 状态机



- **POW 共识机制**
 - 挖矿 (块)



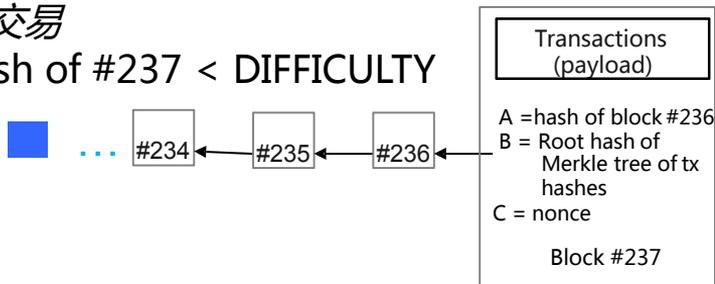
块 #237的矿工 : *Validating (executing) transactions in the payload*
Finding nonces such that
 $h = \text{hash of Block \#237} = \text{SHA256}(A||B||C) < \text{DIFFICULTY}$

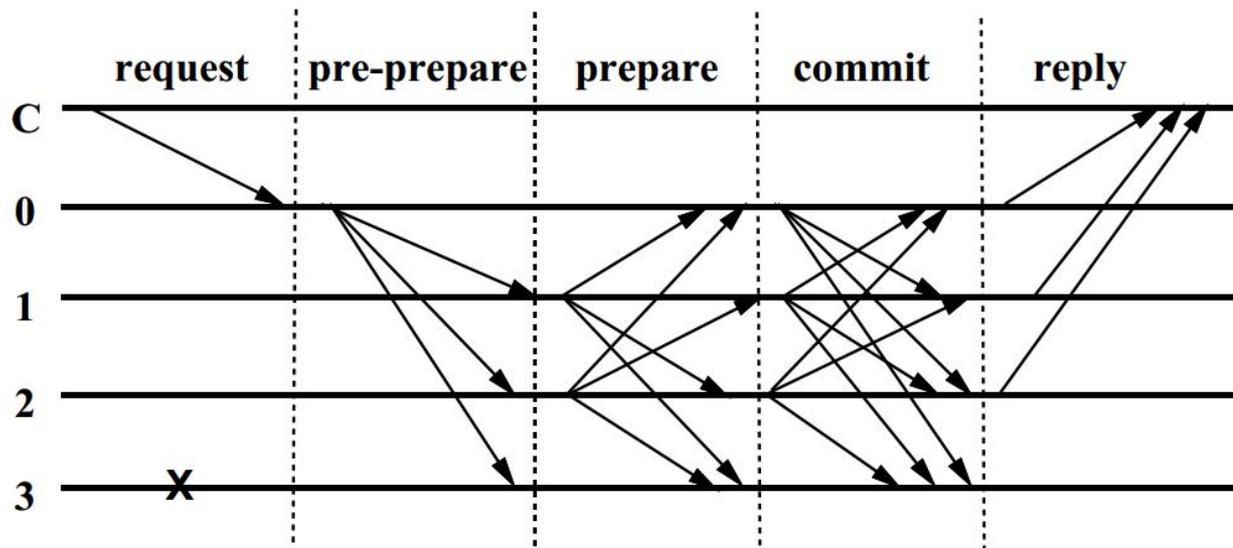
- 块 #237 通过(gossip)传播到网络

在共识 (POW) 之后 , 节点执行智能合约

- **块验证 / 智能合约执行 (每个矿工)**

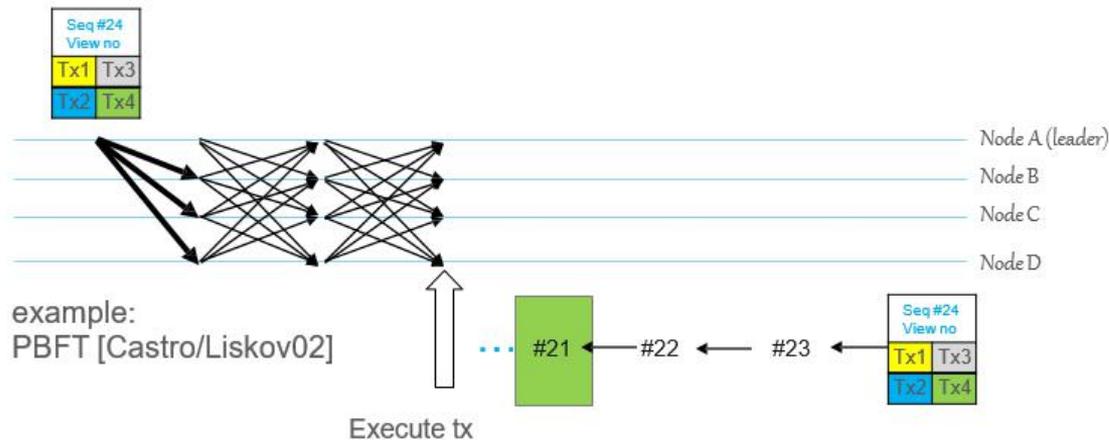
- 验证 (执行) 负荷中的交易
- 验证哈希满足条件 $\text{hash of \#237} < \text{DIFFICULTY}$







联盟链2.0共识--PBFT



- 排序--执行 架构
- 状态机的输入（智能合约的交易）被全部排序
- 共识(排序)后串行执行
- 所有的联盟链都是这么做的, 直到 Fabric v1



先排序再执行的架构

有什么问题吗？

ORDER -> EXECUTE

Agenda

- 区块链简介
- Hyperledger Fabric架构
- Oracle区块链云简介
- Oracle区块链开发

■ 共享账本

- 只可添加的分布式记录系统
- 块 + 状态

■ 智能合约链码 (Chaincode)

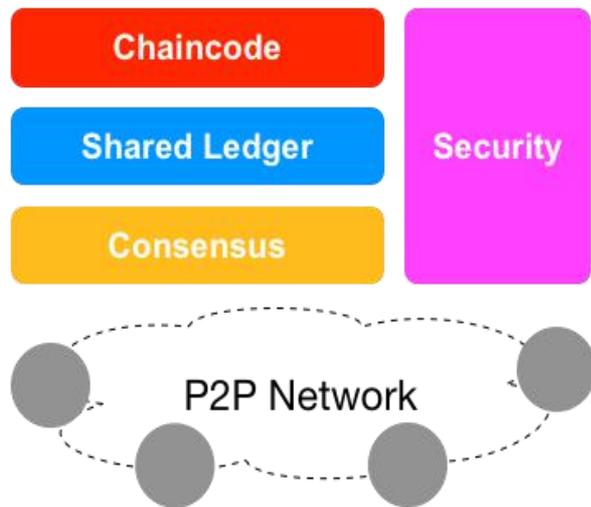
- 交易的商业逻辑
- 无状态和可终止

■ 共识机制

- 验证和排序交易

■ 安全

- 访问控制
- 隐私保护
- 验证
- CA证书



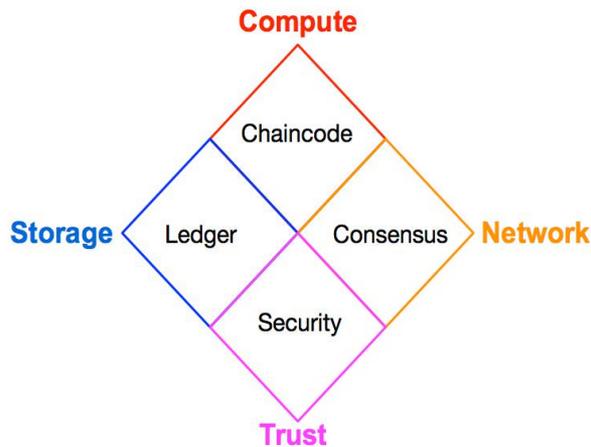


■ 不同密集度的需求/负载

- 链码: **计算** 密集
- 共享账本: **存储** 密集
- 共识机制: **网络** 密集
- 安全: **信任** 密集

■ 解构全功能的节点

- **Endorser**: 背书交易请求
- **Committer**: 写块
- **Orderer**: 只排序, 不管交易内容
- **CA**: 认证管理



■ 全周期验证区块中的交易正确性

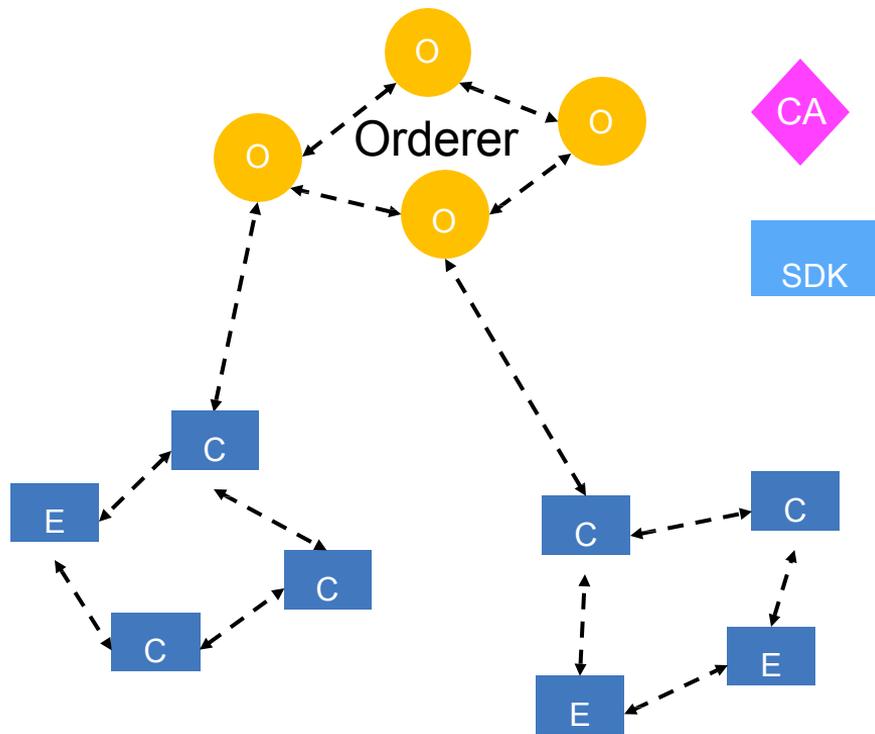
- 背书策略
- 对读写集合的MVCC 多版本系统验证
- 排序
- ACL访问控制

■ 排序节点

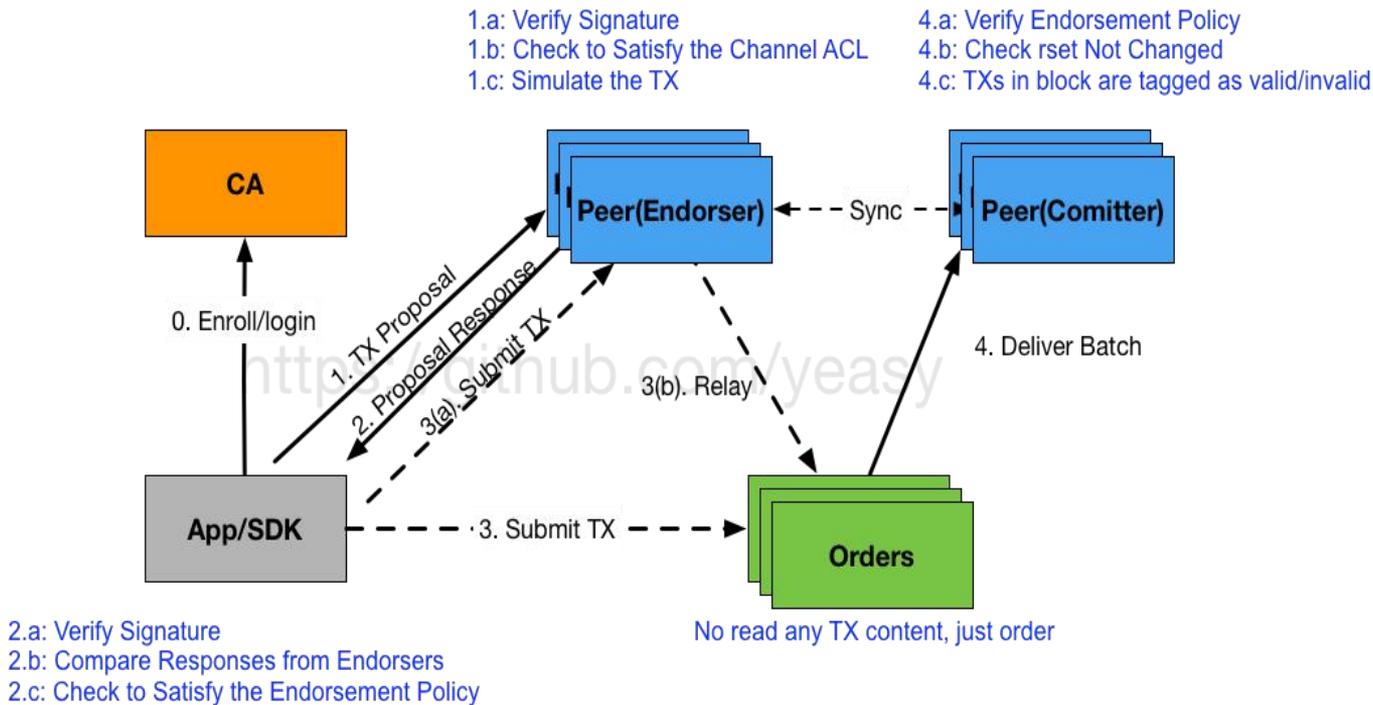
- Solo, Kafka, BFT, ...
- Broadcast(blob), Deliver(seqno, prevhash, blob)



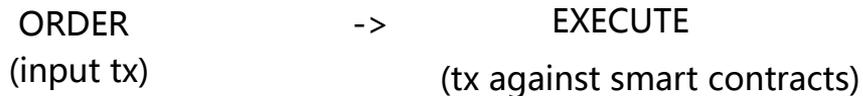
HLF v1 逻辑视图



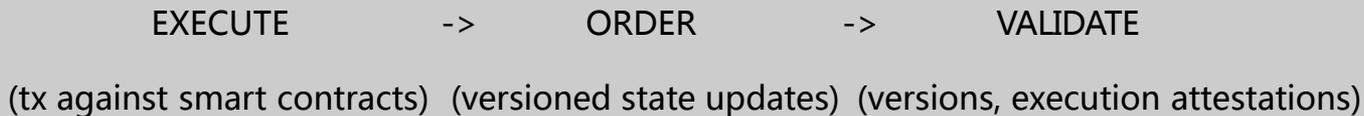
V1 E&C 物理上可以是同一个peer



- 现存的区块链架构



- **Hyperledger Fabric v1 架构**



应用开发者指定两个开发组件:

- 1) 链码 (执行 code)
- 2) 背书策略(验证 code)

- **HLF需求**

- 用通用编程语言写智能合约
- 去掉原生加密货币
- 模块化的共识机制 (不像是其他的联盟链，他们使用特定的共识机制)

所有的联盟链都是

order -> execute

模式

- **这是有问题的:**

- 顺序执行(吞吐量有限, 容易被DoS交易阻塞)
- 所有的节点都要执行所有的智能合约(过于浪费资源)
- 非确定性执行(阻碍一致性, 可能会导致“分叉”)

- 一行说清HLF v1的解决方案:

execute -> order -> validate

联盟链架构 – 彻底重构

- **模块化/可插拔的共识机制**
 - 没有万能的共识机制 (性能, 灵活信任)
- **Execute (链码) - Order (状态更新) - Validate(出块)**
 - 链码不再顺序执行(性能, 扩展性)
 - 不用所有的节点执行所有的链码(有助于保密性, 扩展性)
 - 链码的非确定性执行不再是问题 (一致性, 不分叉)
- **混合的执行模型(结合被动和主动复制)**

Agenda

- 区块链简介
- Hyperledger Fabric架构
- Oracle区块链云简介
- Oracle区块链开发



甲骨文战略：最全面的分布式账本技术云平台

企业就绪

- 许可，高度安全，内置隐私/机密
- 可扩展的业务网络
- 高度灵活的内置备份和可恢复性
- 行业中立



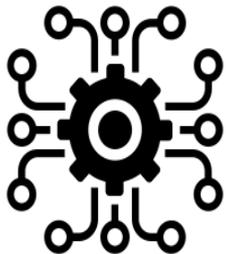
以最短时间实现价值

- 迅速开始开发应用
- API驱动的开发
- 促进新业务流程的快速实验



托管PaaS

- 预装配，随时可用
- 开发人员/集成人员关注交易业务逻辑
- 动态配置，扩展业务网络



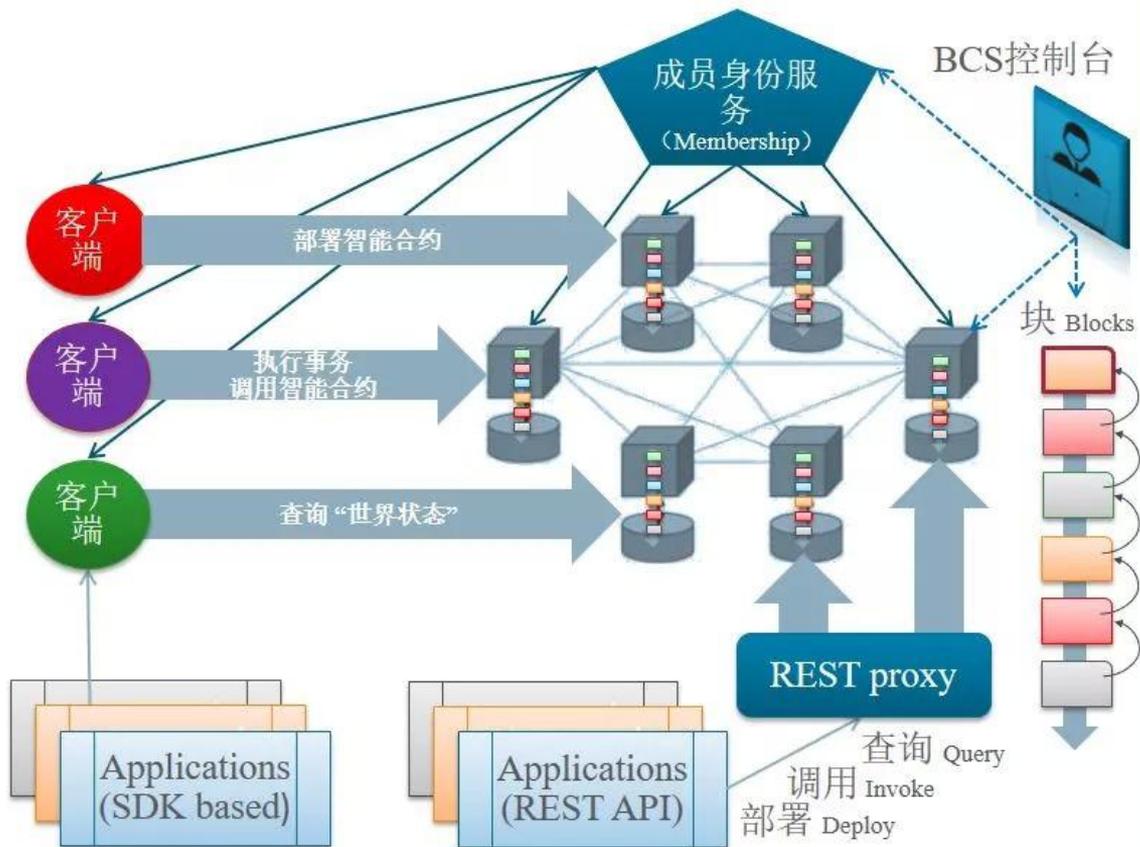
拓展企业边界

- 内置与SaaS、PaaS和本地应用程序的集成
- 安全地扩展与其他组织的可信交易的ERP，SCM和其他业务流程
- 与其他区块链网络交互





Oracle BCS 逻辑视图





甲骨文区块链云服务 采用云原生平台的微服务基础架构

预置系统

托管服务

生产就绪

公有云或私有云

集成服务

针对操作和账本查询/处理的
BCS REST 接口

管理和操作支持 (Ops)

带有 REST 接口的 OPC 操作和 BCS 管理控制台

核心服务

区块链云服务 (BCS) 核心:
节点、智能合约、REST代理、成员服务、排序服务等

数据服务

OPC 存储云 -
对象存储

基础设施服务

OPC & OCM 运行 ACCS (托管的 Docker 容器服务)、IDCS (安全/身份服务)、EHCS (Kafka 服务)

Public Cloud

IaaS, SaaS, PaaS



Cloud@Customer

Cloud Machines





区块链云服务交互-管理/操作

- 区块链云服务控制台

- 提供网络用户界面和REST 接口 用于 管理、操作和监控区块链网络

- 管理内容

- 网络
- 节点
- 通道 / 账本
- 智能合约

The screenshot displays two screenshots of the Oracle Blockchain Cloud Service Console. The top screenshot shows the 'Node Management' page with a table of nodes:

Node Name	Routes	Type	Status	Actions
peer1	gRPC grpcs://peer0.org1.example	Peer	activating	[Stop] [Start] [Refresh]
orderer1	gRPC grpcs://orderer.example.co	Orderer	up	[Stop] [Start] [Refresh]

The bottom screenshot shows the 'Channel Management' page with a table of channels and chaincodes:

Name	Version	Type	Actions
mychannel		Channel	
end2end	v1	Chaincode	Upgrade
channel1		Channel	
obcs-sample-example02	obcs-sample-v0	Chaincode	Upgrade
obcs-sample-marbles	obcs-sample-v0	Chaincode	Upgrade
channel2		Channel	
end2end-3	v1	Chaincode	Upgrade

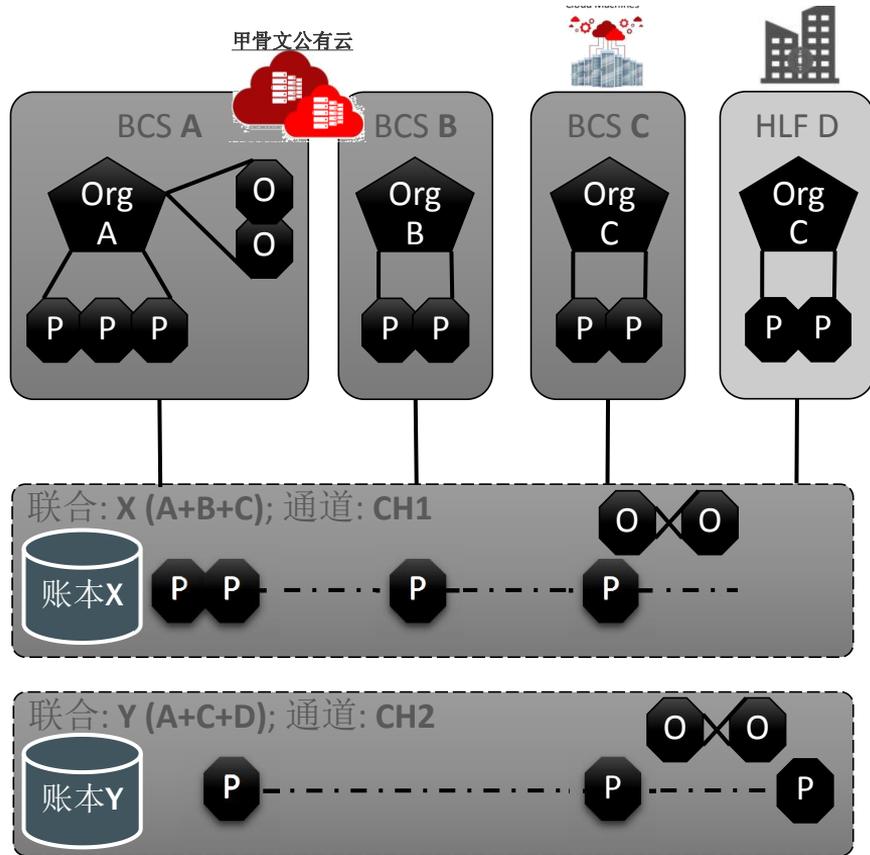
On the right side of the Channel Management page, there is a 'mychannel LEDGER' section with five circular gauges showing: 5 Blocks, 0.08 Block Speed, 4 Transaction Deployments, 2 Invokes, and 2 Invokes. Below this is a 'Query Ledger' section with a table of ledger entries:

Block #	Time	Deployments	Invocations
4	2017-06-26 23:27:48	0	1
3	2017-06-26 23:27:46	1	0
2	2017-06-26 23:27:36	0	1



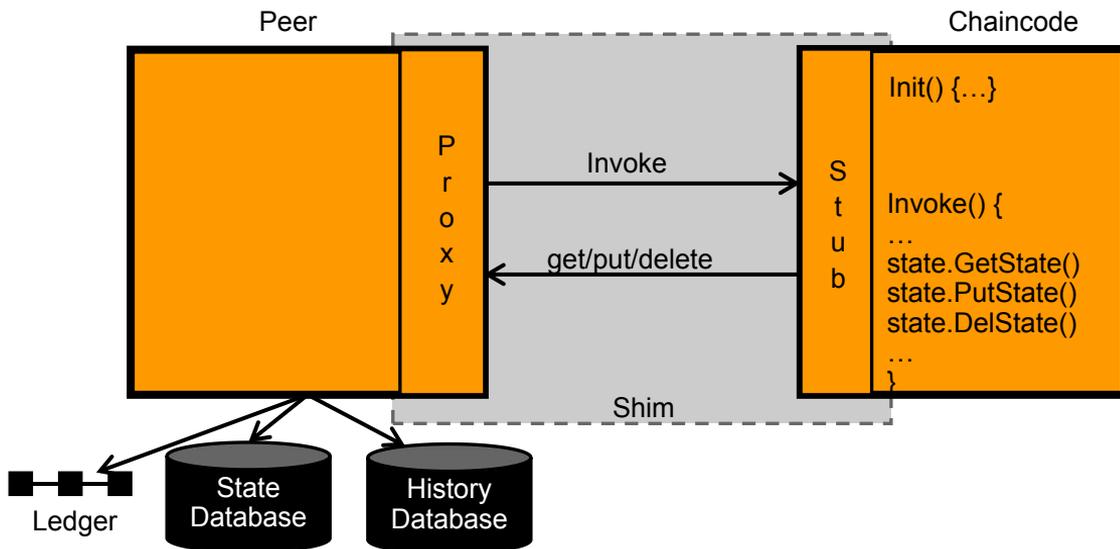
区块链云服务交互- 创建业务网络

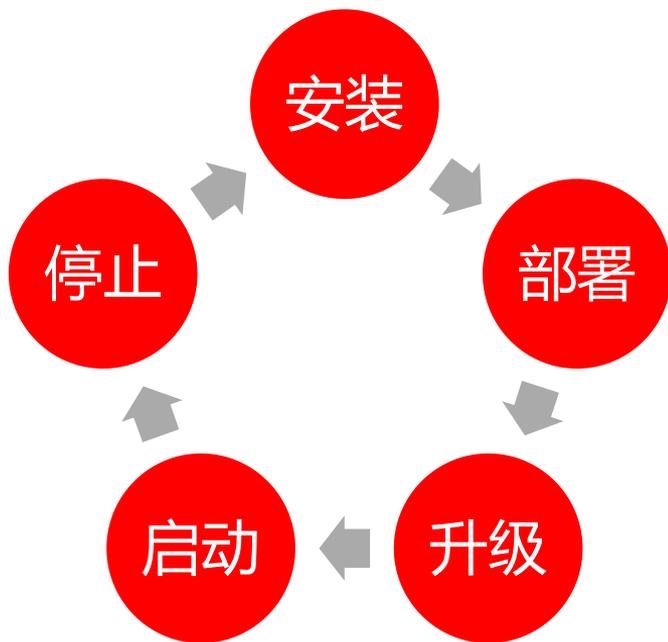
- 组织间合作网络使用一个共同的区块链
 - 甲骨文云或异构节点
- 创建一个新的网络或添加到现有网络
- 通过创建具有独特策略和跨多组织数据接入的通道确保隐私



Agenda

- 区块链简介
- Hyperledger Fabric架构
- Oracle区块链云简介
- Oracle区块链开发





账本状态(State)读写

- GetState(key string) ([]byte, error)
- PutState(key string, value []byte) error
- GetStateByRange(startKey, endKey string) (StateQueryIteratorInterface, error)
- GetHistoryForKey(key string) (StateQueryIteratorInterface, error)
- GetQueryResult(query string) (StateQueryIteratorInterface, error)



Chaincode执行必须是确定性的

- 只依赖state数据库,其它数据通过参数传入
- 不要使用 时间戳, 主机名, 本地环境等
- 避免调用外部服务

要小心依靠查询的结果

- 其他的交易有可能插入或更新key, 可能导致验证或背书错误

甲骨文区块链云服务 总结

简化配置和管理

- 快速个性化配置
- 简化操作的监控面板

快速应用开发和集成

- 通过简单的REST调用实现集成
- 与甲骨文其它云服务的无缝集成

更安全更私密

- 与IDCS集成，提供基于角色的授权服务
- 账本数据加密

快速拓展网络

- 创建拥有多个BCS实例的网络
- 私有通道

更高灵活性、可用性、 可伸缩性

- 完整而连续的账本备份；自动化账本恢复；补丁和升级
- 可扩展的成员加入服务；按需、自动化的纵向/横向扩展